NEAT EVALUATION FOR UNISYS:

Attack Surface Management

Market Segment: Overall

Introduction

This is a custom report for Unisys presenting the findings of the 2025 NelsonHall NEAT vendor evaluation for *Attack Surface Management* in the *Overall* market segment. It contains the NEAT graph of vendor performance, a summary vendor analysis of Unisys for attack surface management services, and the latest market analysis summary.

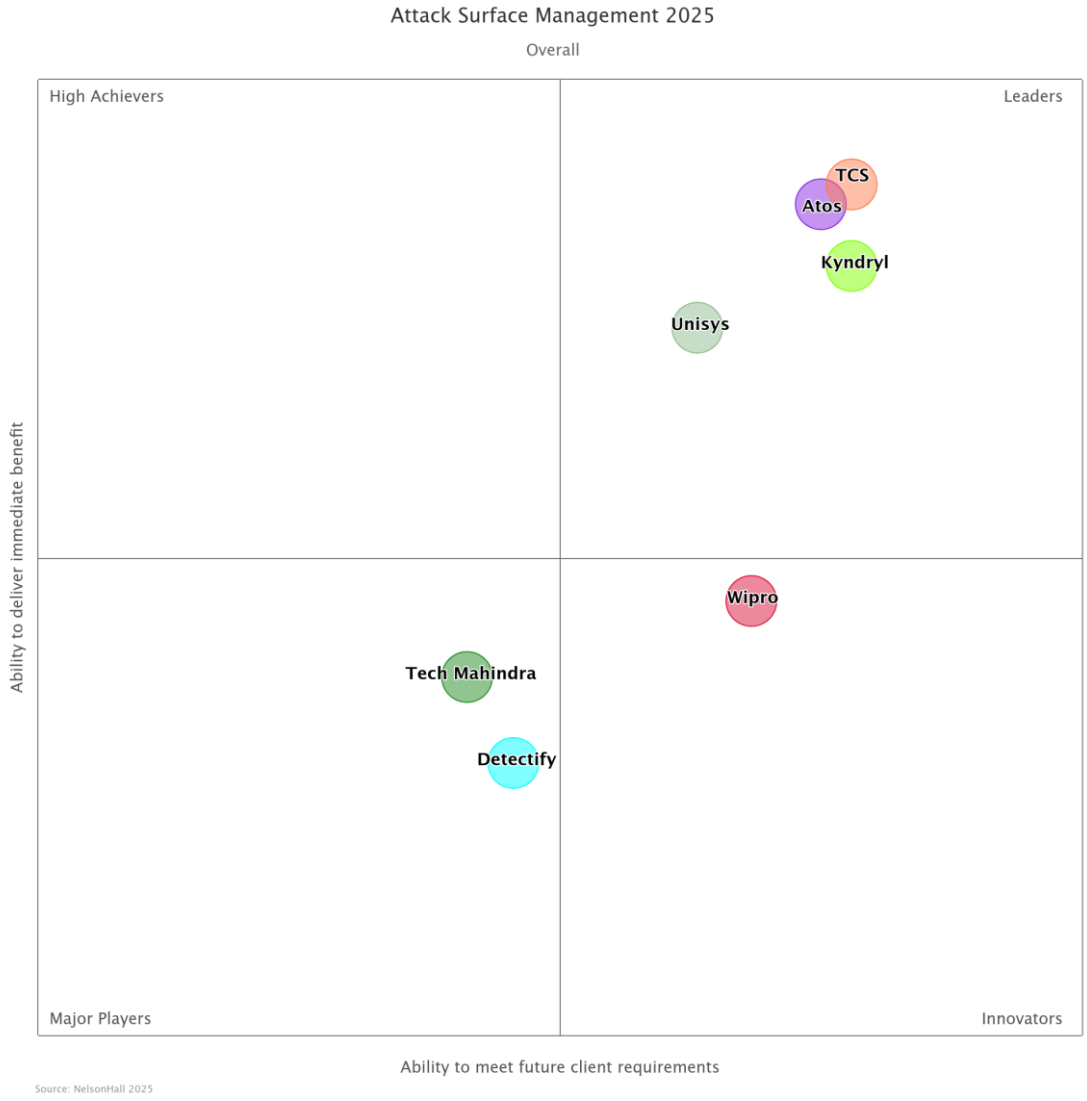
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering attack surface management (ASM) as part of their cyber resiliency services. The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors overall, and with specific capability in automated ASM services and integrating ASM within a wider cyber resiliency strategy.

Evaluating vendors on both their 'ability to deliver immediate benefit' and their 'ability to meet future client requirements', vendors are identified in one of four categories: Leaders, High Achievers, Innovators, and Major Players.

Vendors evaluated for this NEAT are: Atos, Detectify, Kyndryl, TCS, Tech Mahindra, Unisys, and Wipro.

Further explanation of the NEAT methodology is included at the end of the report.

NEAT Evaluation: Attack Surface Management (Overall)



NelsonHall has identified Unisys as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects Unisys' overall ability to meet future client requirements as well as delivering immediate benefits to its cyber resiliency clients.

Leaders are vendors that exhibit both a high capability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet future client requirements.

Buy-side organizations can access the *Attack Surface Management* NEAT tool (*Overall*) here.

Vendor Analysis Summary for Unisys

Overview

Unisys groups attack surface management under Continuous Threat Exposure Management (CTEM) services. These services look to gain continuous visibility into the organization's attack surface through the use of security tooling and services. Primarily, CTEM services aim to:

- Monitor the digital enterprise for risks
- Assess the impacts of threats on business
- Prioritize risks based on the business context
- Mitigate by focusing on the most critical threats first
- Evaluate defenses using simulated attacks
- Monitor compliance and regulatory requirements
- Improve practices, processes, and technologies
- Adapt cybersecurity strategies to defend businesses from emerging threats and vulnerabilities.

Unisys leads with spiderSilk to perform external attack surface management to detect unknown assets and potential threat vectors; these engagements can begin using only the organization's name. This external ASM returns domains, DNS records, hosting providers, and SSL, TLS and other certificates. Additionally, in support of external attack surface management, Unisys monitors ~800 forums and telegram channels across different languages to detect exposed business-related data and GitHub scans to identify leaked source codes or API keys. Secondly, Unisys innovates with KeyCaliber's Continuous Threat Exposure Management platform for internal attack surface management to identify the criticality of assets and map assets to applications and business processes.

Unisys performs security testing, including white, grey, and black box penetration testing, leading with Cobalt penetration testing as a service platform, and manual testing using Unisys' attack playbooks with best-of-breed solution partners.

It prices its security testing, including penetration testing, on a fixed-price basis based on the scope of the testing. For support in delivering manual penetration testing services, the company leverages partnerships with several penetration-testing-focused vendors capable of augmenting delivery talent both on- and offshore along with Unisys-badged cybersecurity experts. Unisys does not currently offer automated red teaming; however, the company is evaluating automated red teaming platform providers.

Financials

Unisys' Cloud, Applications & Infrastructure Solutions (CA&I) revenue for CY 2024 is estimated to be ~$530m. The company does not release revenue figures for its cyber resiliency or attack surface management services. However, NelsonHall estimates Unisys' 2024 ASM revenues were $25m.

The ASM revenue breakdown by region in 2024 is estimated to be: North America 48%, Latin America 28%, EMEA 11%, Asia Pacific 13%.

Strengths

- Unisys is using some of the best-of-breed platforms to offer external and internal ASM services
- It augments these best-of-breed platforms with AI labeling of attributes and manual verification to reduce false positives
- Supporting clients with a wide array of cyber resiliency and IT services.

Challenges

- Unisys is not relating cybersecurity risk to financial risk, though it had previously aimed to do so through its TrustCheck offering. Instead, the company is leading with KeyCaliber's capabilities to estimate the criticality of the cyber risk on a 1-100 score
- It does not currently offer automated teaming/penetration testing of detected vulnerabilities that could improve risk validation and qualification, or breach simulation to help clients in understanding the cyber kill chain and evaluate the current security controls
- Unisys lacks automated continuous compliance support. While this can be assessed intermittently, a lack of continuous assessment reduces the effectiveness of these services as they do not capture more frequent changes to the attack surface.

Strategic Direction

The majority of Unisys' attack surface management and wider cyber resiliency clients are usually engaged as part of a larger outsourcing contract beyond cyber resiliency, such as digital workspace or infrastructure services. Unisys has begun offering its cyber resiliency services through the Azure and AWS marketplaces and government frameworks and this has resulted in more isolated cyber resiliency contracts.

Unisys has stated that it intends to open a CoE designed to accelerate the continuous transformation of service delivery and SOPs that will, in part, include ASM services. Additionally, it is dedicating efforts towards internal education via technology and solution hands-on training sessions for CTEM solutions.

Unisys has a detailed roadmap of the services it intends to add to its attack surface management and overall cyber resiliency portfolios. This roadmap includes:

- The introduction of penetration testing as-a-Service and exploring the option of adding a bug bounty program
- Adding quantum risk assessments to assess clients' current levels of cryptology against quantum attacks, to support these clients in understanding what can be done now to reduce the opportunity to steal data, and to implement roadmaps to support organizations in becoming resistant
- Adding breach attack simulation and automated red teaming following the discovery of risks
- Supporting the ability to rate a client's security posture against industry peers
- Relaunching its digital forensics services

- Evaluating continuous compliance monitoring products and third parties to offer white labeled compliance services
- AI-powered third-party risk assessments
- Attack surface management of AI models. As yet, none of Unisys' clients are specifically asking for support with regard to securing AI models; for example, implementations of OpenAI. However, Unisys believes that clients are primed to start these engagements and the company is currently lining up partners in this area.

Outlook

Unisys provides ASM through its Continuous Threat Exposure Management (CTEM) services. It is using spiderSilk and KeyCaliber platforms for external and internal ASM respectively, with Unisys providing additional AI labeling of attributes and manual verification to reduce the number of false positives detected by these platforms. This manual verification alongside additional penetration testing and red teaming of risks accounts for more than a quarter of Unisys' CTEM revenues.

Unisys is working to improve its other ASM services; the company is currently lacking in automated continuous compliance, digital risk protection, and automation within its ASM services. This is part of its 2025 roadmap.

As the majority of Unisys' cyber resiliency and ASM services are clients of wider IT services contracts and benefit from Unisys' business knowledge to assign business risks, organizations that are seeking ASM services as part of a wider contract should consider Unisys.

Attack Surface Management Market Summary

Overview

Attack Surface Management is the process of identifying and managing cybersecurity vulnerabilities within systems, networks, and applications. These ASM services include asset discovery, vulnerability assessments, prioritization, monitoring, remediation, penetration testing, red teaming, brand monitoring, third-party risk management, and digital risk protection reporting.

ASM providers include IT services vendors, network communication providers, ASM platform owners, and consultancies.

BFSI is the largest vertical market for ASM, as it is in the wider cyber resiliency market, due to the increased regulatory requirements facing these organizations. Similarly, within healthcare, regulations like HIPAA have driven data security requirements; these requirements will increase over time as the amount of patient data increases, and as organizations that interact with healthcare data (such as medical device companies) are mandated to create and maintain SBOMs.

Governments and critical infrastructure companies in energy & utilities have had similar requirements for some time; as national security concerns increase, increased defense spending will be mirrored in increased ASM spending.

Manufacturing growth will be supported by increased use of ASM to detect and secure OT and supply chains. Similarly, retail growth will be supported by supply chain third and fourth parties.

Buy-Side Dynamics

Organizations face the following key challenges in managing their attack surface:

- Ongoing asset sprawl, increasing the number of platforms, applications, and technologies in use
- The absence of a single source of truth for an organization’s asset inventory increases the difficulty in securing and remediating vulnerabilities
- Inadequate AppSec and vulnerability management programs that cannot detect or manage the high number of vulnerabilities within assets
- An inability to understand which vulnerabilities pose the greatest threats that can be prioritized. Solutions that do consider rating the criticality of the risk often fail to consider the importance of the asset to the business or fail to rate risks associated with users' access to systems and data. An increased focus on users as part of ASM lends itself to measuring the effectiveness of zero-trust roll outs
- Brand monitoring being slow to detect changes
- Regulatory requirements, depending on the organization’s industry and the regions in which it operates, to build and manage SBOMs, or more generally secure data and assets
- The need to integrate security best practices into application development, not only to build SBOMs, but to follow DevSecOps practices to reduce vulnerabilities, ensure compliance, and improve overall cyber resiliency

- A high number of third and fourth parties that can pose vulnerabilities to the organization, with difficulties in building a vendor inventory
- The typical way of investigating the risk associated with third parties are questionnaires which are inadequate point-in-time light-touch assessments.

Market Size & Growth

The global ASM market (including both platforms and services) was worth $9bn in 2024, and is estimated to be $11.25bn in 2025. It will grow at 15.5% CAGR to reach $20bn by 2028.

Market growth in the U.S. will be boosted by the likes of CISA directives; for example, for the creation of SBOMs and the need to follow digital adoption that leverages a relatively higher number of cloud, IoT, and similar technologies.

Toward the end of the 2025-2028 period, technology adoption such as GenAI, especially in geographies that are more likely to have regulatory requirements such as the EU, will increase the pressure on ASM requirements. Similarly, quantum computing will increase the need for ASM towards the end of the period as traditional encryption methods will become less adequate as a barrier towards data exfiltration.

Success Factors

Critical success factors for vendors within the attack surface management market are:

- The ability to work across the client's business operations, IT, and third parties
- The ability to detect assets within an organization, the configurations, and then verify these assets to build and maintain a single source of truth that can be used in vulnerability management programs
- Best-of-breed selection of tools to detect these assets and then perform vulnerability assessments and an adequate scale within penetration testing to support logical testing that cannot be automated
- An understanding of the client organization that can be used alongside vulnerability data to adequately judge the risk of the vulnerability to the organization and prioritize remediation of these vulnerabilities in a manner that addresses the largest and most immediate risks to the business
- The ability to monitor the performance of zero trust and data security protocols as part of a wider ASM program to understand what data exists, on what platforms it resides, and what access to the data there is, both from humans and machines
- Continuous brand monitoring, including on the deep and dark web to detect items such as leaked credentials before they are used
- Keeping abreast of the regulatory requirements, understanding the risks posed to the client in not meeting these requirements, and supporting the organization in meeting and monitoring adherence
- Tooling and best-practice support to embed DevSecOps within application development so the organization can increase the overall security of the applications and maintain an SBOM that can be used to monitor cyber resiliency against zero-day attacks

- Tooling and support to identify and investigate risks posed by third and fourth parties, extending beyond simple questionnaires of security posture to a minimum level of third-party brand monitoring.

Outlook

Over the next five years, NelsonHall expects to see:

- A higher percentage of automation in penetration testing
- ASM platforms with more connections to data discovery, IAM, and SAST/DAST/SOAR platforms to detect more risks and manage detected risks
- Threat hunting and deep/dark web monitoring will become standard services in each ASM engagement, similar to threat intelligence gathering. Threat hunting will also start to consider supply chain/third-party attacks and attacks on ML datasets
- Third-party risk management will be extended into fourth-party risk management (i.e. the third parties of third parties)
- Organizations will also move beyond simple questionnaire assessments for third parties of mid to high importance, instead requiring external assessment, penetration testing, and code reviews performed by independent third-party security firms to better measure the security posture of these firms
- Social engineering will combine with ID-ASM efforts to educate users to avoid cyber attacks
- Identity ASM (ID-ASM) to become a recognized service for integrating ID governance, PAM, and asset management systems.

NEAT Methodology for Attack Surface Management

NelsonHall's (vendor) Evaluation & Assessment Tool (NEAT) is a method by which strategic sourcing managers can evaluate outsourcing vendors and is part of NelsonHall's *Speed-to-Source* initiative. The NEAT tool sits at the front-end of the vendor screening process and consists of a two-axis model: assessing vendors against their 'ability to deliver immediate benefit' to buy-side organizations and their 'ability to meet future client requirements'. The latter axis is a pragmatic assessment of the vendor's ability to take clients on an innovation journey over the lifetime of their next contract.

The 'ability to deliver immediate benefit' assessment is based on the criteria shown in Exhibit 1, typically reflecting the current maturity of the vendor's offerings, delivery capability, benefits achievement on behalf of clients, and customer presence.

The 'ability to meet future client requirements' assessment is based on the criteria shown in Exhibit 2, and provides a measure of the extent to which the supplier is well-positioned to support the customer journey over the life of a contract. This includes criteria such as the level of partnership established with clients, the mechanisms in place to drive innovation, the level of investment in the service, and the financial stability of the vendor.

The vendors covered in NelsonHall NEAT projects are typically the leaders in their fields. However, within this context, the categorization of vendors within NelsonHall NEAT projects is as follows:

- Leaders: vendors that exhibit both a high capability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet future client requirements
- High Achievers: vendors that exhibit a high capability relative to their peers to deliver immediate benefit but have scope to enhance their ability to meet future client requirements
- Innovators: vendors that exhibit a high capability relative to their peers to meet future client requirements but have scope to enhance their ability to deliver immediate benefit
- Major Players: other significant vendors for this service type.

The scoring of the vendors is based on a combination of analyst assessment, principally around measurements of the ability to deliver immediate benefit; and feedback from interviewing of vendor clients, principally in support of measurements of levels of partnership and ability to meet future client requirements.

Note that, to ensure maximum value to buy-side users (typically strategic sourcing managers), vendor participation in NelsonHall NEAT evaluations is free of charge and all key vendors are invited to participate at the outset of the project.

Exhibit 1

'Ability to deliver immediate benefit': Assessment criteria

Assessment Category	Assessment Criteria
Offerings	Compliance and regulatory monitoring Risk scoring and prioritization Risk remediation Penetration testing/red teaming Brand monitoring Third-party risk management Threat intelligence Threat hunting Internal Attack Surface Management External Attack Surface Management Application scanning
Delivery Capability	Manual attack surface management capability Automated external attack surface management capability Tooling in support of DevSecOps Use of security accelerators, templates, custom queries
Benefits Achieved	Asset visibility Identification of risks Identification and management of third-party risks Proactive threat mitigation Reporting and dashboards available to clients Reduction in the number of incidents Ability to support the meeting of related regulations Continuous understanding of cyber risk

Exhibit 2

'Ability to meet client future requirements': Assessment criteria

Assessment Category	Assessment Criteria
Service Innovation Culture	Investment in threat intelligence and hunting
	Investment in internal attack surface management
	Investment in external attack surface management
	Investment in automation within ASM
	Investment in scoring and managing risks
	Investment in third-party risk management
	Investment in tooling in support of DevSecOps

For more information on other NelsonHall NEAT evaluations, please contact the NelsonHall relationship manager listed below.

research.nelson-hall.com

Sales Inquiries

NelsonHall will be pleased to discuss how we can bring benefit to your organization. You can contact us via the following relationship manager:

Darrin Grove at darrin.grove@nelson-hall.com